REMARKS

In the Official Action mailed **26 August 2005**, the Examiner reviewed claims 1-5, 7-13, 15-21, and 23-48. Claims 1-5, 7-13, 15-21, and 23-48 were rejected under 35 U.S.C. §103(a) as being unpatentable over O'Flaherty et al (USPN 6,275,824, hereinafter "O'Flaherty") in view of Sweet et al (USPub 2002/0031230, hereinafter "Sweet").

Rejections under 35 U.S.C. §103(a)

Independent claims 1, 9, 17, 25, 33, and 41 were rejected as being unpatentable over O'Flaherty in view of Sweet.

Applicant respectfully points out that O'Flaherty teaches a system in which information is held in a database for use in data storage and retrieval operations (see O'Flaherty, Abstract and FIG. 5). The data base in O'Flaherty supports blocking certain data from outside retrieval (see O'Flaherty, col. 8, lines 16-24 and FIG. 11, elements 260, 264, and 266). There are two methods for modifying the private data in the O'Flaherty database. The first relies on a "privacy administrator" (see O'Flaherty, col. 12, lines 30-43). The second allows a user to modify the information in the database (see O'Flaherty, col. 12, lines 50-54).

Sweet teaches a system for securing the transmission of information in documents (see Sweet, Abstract and FIG. 2). For example, the system proposed by Sweet allows a group to send a single document with several different parts of the document encrypted so that only certain members of the receiving group can decrypt and read the document (see Sweet, paragraph [0014]). In order to manage the security and access level of users, Sweet proposes a hierarchical command structure (see Sweet, paragraph [0035]). The command structure includes a high-level security officer (SO), a domain administrator (DA), and a layer of workgroup administrators (WA). The DAs and the SO are responsible for defining security policy on the network, and determining access standards, among other roles (see Sweet paragraphs [0091]-[0102] and FIG. 2). The WA manages workgroups;

including assigning, distributing, and updating member security profiles (see Sweet, paragraph [0106]-[0110]). All of these actors have access to secured information (the security profiles) as Sweet does not explicitly limit any actor's access.

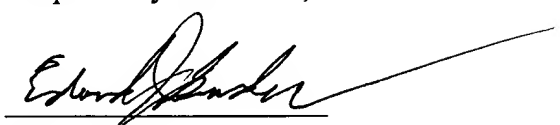
In contrast, the present invention limits the actor's access based upon the actor's classification (see FIG. 1 and page 8, lines 9-20 of the instant application). There nothing in the systems of O'Flaherty and Sweet, either separately or in combination, which suggests limiting the actor's access based upon the actor's classification. Applicant respectfully requests the Examiner to point out specifically where within O'Flaherty and/or Sweet there is a suggestion to limit any actor's access to the security profiles.

Applicant respectfully submits that independent claims 1, 9, 17, 25, 33, and 41 as presented are in condition for allowance. Applicant also submits that claims 2-5 and 7-8, which depend upon claim 1, claims 10-13 and 15-16, which depend upon claim 9, claims 18-21 and 23-24, which depend upon claim 17, claims 26-32, which depend upon claim 25, claims 34-40, which depend upon claim 33, and claims 42-48, which depend upon claim 41, are for the same reasons in condition for allowance and for reasons of the unique combinations recited in such claims.

CONCLUSION

It is submitted that the present application is presently in form for allowance. Such action is respectfully requested.

Respectfully submitted,

By 

Edward J. Grundler
Registration No. 47,615

Date: 25 October 2005

Edward J. Grundler
PARK, VAUGHAN & FLEMING LLP
2820 Fifth Street
Davis, CA 95616-7759
Tel: (530) 759-1663
FAX: (530) 759-1665
Email: edward@parklegal.com